



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,817	12/12/2003	Bernard D. Aboba	13768.432.1	3500

47973 7590 08/22/2007
WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER

JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

08/22/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

1. This action is responding to application papers filed on **12-12-2003**.
2. Claims **1 - 40** are pending. Claims **1, 10, 19, 24, 29, 35** are independent.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim **1 - 40** are rejected under 35 U.S.C. 102(e) as being anticipated by **Whelan et al.** (US PG PUB No. **20040198220**).

Regarding Claims 1, 10, Whelan discloses in a station, computer program product that is capable of communicating with at least one access point in a communications network, a method for creating a secure association between the station and at least one access point, the method comprising:

- a) obtaining discovery information from one or more access points in the communications network, the discovery information reflecting capabilities of the one or more respective access points to facilitate communication with the station;

(see Whelan paragraph [0049], lines 1-10: detect (discover) information obtained from access points)

- b) selecting one of the access points to become associated with; (see Whelan paragraph [0049], lines 10-12: placed on associated list)
- c) authenticating the selected access point; (see Whelan paragraph [0054], lines 1-4; paragraph [0026], lines 1-4: authenticate access point (mobile device))
- d) sending a discovery verification request to the selected access point for the discovery information of the selected access points to be verified; (see Whelan paragraph [0013], lines 3-7: request for verification; paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authenticate access point) and
- e) receiving an acknowledgement receipt from the selected access point verifying the discovery information. (see Whelan paragraph [0013], lines 7-10: receive response, verify information)

Regarding Claims 2, 11, Whelan discloses a method, computer program product as recited in claims 1, 10, wherein the discovery verification request includes an identifiable security object obtained during authentication. (see Whelan paragraph [0013], lines 3-7: authentication request; paragraph [0076], lines 1-3: certificate, security object)

Regarding Claims 3, 12, Whelan discloses a method, computer program product as recited in claims 2, 11, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number. (see Whelan paragraph [0076],

lines 1-3: certificate, security object)

Regarding Claims 4, 13, Whelan discloses a method, computer program product as recited in claims 1, 10, wherein authenticating the access point includes identifying a certificate from a trusted certificate authority. (see Whelan paragraph [0096], lines 1-3; paragraph [0076], lines 3-5: certificate authority (CA) utilized for authentication)

Regarding Claims 5, 14, Whelan discloses a method, computer program product as recited in claims 4, 13, wherein the trusted certificate authority is a server of the communications network. (see Whelan paragraph [00076], lines 3-5: CA is a server)

Regarding Claims 6, 15, Whelan discloses a method, computer program product as recited in claims 1, 10, wherein authenticating the access point is part of a mutual authentication that also involves the access point authenticating the station. (see Whelan paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: mutual authentication)

Regarding Claims 7, 16, Whelan discloses a method, computer program product as recited in claims 1, 10, further including an act of sending a frame to the access point after receiving the acknowledgment receipt, wherein the frame includes a verifiable key that indicates to the access point that the frame is actually received from the station. (see Whelan paragraph [0094], lines 1-3: shared secret key utilized to exchange messages)

Regarding Claims 8, 17, Whelan discloses a method, computer program product as recited in claim 7, wherein the frame includes a management frame configured to control the secure association between the access point and the station. (see Whelan paragraph [0094], lines 1-3: secure exchange of messages between mobile units (access point and station))

Regarding Claims 9, 18, Whelan discloses a method, computer program product as recited in claims 8, 16, wherein the management frame is configured to terminate the secure association. (see Whelan paragraph [0030], lines 1-5; paragraph [0030], lines 17-20: excluded list (terminate association))

Regarding Claims 19, 24, Whelan discloses in an access point that is capable of communicating with at least one station in a communications network, a method for creating a secure association between the station and at least one access point, the method comprising:

- a) providing discovery information to the station, the discovery information reflecting capabilities of the access point to facilitate communication with the station; (see Whelan paragraph [0049], lines 1-10: provide (discovery) information obtained from access points)

- b) providing a certificate with the discovery information that is used by the station to authenticate the access point; (see Whelan paragraph [0096], lines 1-3: certificate utilized in authentication)
- c) receiving a discovery verification request from the station for the discovery information to be verified; (see Whelan paragraph [0013], lines 3-7: request for discovery security information) and
- d) verifying the discovery verification request to the station. (see Whelan paragraph [0013], lines 7-10: response to request, verification discovery security information)

Regarding Claims 20, 25, Whelan discloses a method, computer program product as recited in claims 19, 24, wherein the discovery verification request includes an identifiable security object obtained during authentication of the access point by the station. (see Whelan paragraph [0076], lines 3-5; paragraph [0096], lines 1-3: certificate, security object)

Regarding Claims 21, 26, Whelan discloses a method, computer program product as recited in claims 20, 25, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number. (see Whelan paragraph [0076], lines 3-5; paragraph [0096], lines 1-3: security object, certificate)

Regarding Claims 22, 27, Whelan discloses a method, computer program product as

Art Unit: 2136

recited in claims 19, 24, wherein the certificate is signed by a server of the communications network. (see Whelan paragraph [0096], lines 1-3: CA, server system, certificate signed by CA)

Regarding Claims 23, 28, Whelan discloses a method, computer program product as recited in claims 19, 24, further including an act of authenticating the station as an authorized network device. (see Whelan paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authentication, mobile unit)

Regarding Claims 29, 35, Whelan discloses in a first network device that is engaged in a secure association with a second network device in a communications network, a method for verifying management frames transmitted between the network devices, the method comprising:

- a) at the first network device creating a management frame configured to control the secure association; (see Whelan paragraph [0030], lines 1-5: secure association information)
- b) at the first network device attaching a verifiable key to the management frame; (see Whelan paragraph [0094], lines 1-3: shared secret key (verifiable key)) and
- c) at the first network device sending the management frame with the verifiable key to the second network device, wherein upon receiving the management frame and the verifiable key, the second network device recognizes the verifiable key and verifies the management frame prior to executing the management frame.

Art Unit: 2136

(see Whelan paragraph [0094], lines 1-3: secure communication, shared secret key utilized for message encryption)

Regarding Claims 30, 36, Whelan discloses a method, computer program product as recited in claims 29, 35, wherein at least one of the first and second network devices is a station configured to access the network and wherein at least one of the first and second network devices is an access point configured to provide the station access to the communications network. (see Whelan paragraph [0003], lines 4-6: access point, provide access to network communications)

Regarding Claims 31, 37, Whelan discloses a method, computer program product as recited in claims 30, 36, wherein the first network device is a mobile and wireless communications device. (see Whelan paragraph [0002], lines 12-16: mobile unit (mobile device))

Regarding Claims 32, 38, Whelan discloses a method, computer program product as recited in claims 29, 35, wherein the verifiable key is a provided by a server of the communications network. (see Whelan paragraph [0076], lines 1-5: paragraph [0096], lines 1-3: certificate, encryption key (PKI) provided by a server)

Regarding Claims 33, 39, Whelan discloses a method, computer program product as recited in claim 29, wherein the verifiable key comprises a derivative of a key formed

during authentication of at least one of the first and second network devices. (see Whelan paragraph [0094], lines 1-3: secure communications key, shared secret key)

Regarding Claims 34, 40, Whelan discloses a method, computer program product as recited in claims 29, 35, wherein prior to sending the management frame, the method includes creating the secure association, and wherein creating a secure association includes the first network device:


- a) obtaining discovery information from the second network device, the discovery information reflecting capabilities of the second network device to facilitate communication between with the first network device and the network; (see Whelan paragraph [0049], lines 1-10: detect (discover) information obtained from access points)
- b) authenticating the second network device; (see Whelan paragraph [0054], lines 1-4; paragraph [0026], lines 1-4: authenticate access point (mobile device))
- c) sending a discovery verification request to the second network device for the discovery information of the second network device to be verified; (see Whelan paragraph [0013], lines 3-7: request for verification; paragraph [0009], lines 1-3; paragraph [0054], lines 1-4: authenticate access point) and
- d) receiving an acknowledgement receipt from the second network device verifying the discovery information. (see Whelan paragraph [0013], lines 7-10: receive response, verify information)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


CVJ
June 25, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


7, 9, 07

Carlton V. Johnson
Examiner
Art Unit 2136